

WHAT IS CLAIMED IS:

1 1. A cryptographic communication method wherein when
2 different encryption algorithms are operated at a
3 transmission side and a reception side, the transmission
4 side encrypts an encryption algorithm operated at the
5 transmission side with an encryption algorithm operated at
6 the reception side and transmits the encrypted algorithm to
7 the reception side.

1 2. A cryptographic communication method wherein information
2 on an encryption algorithm operated at a transmission side
3 and information on an encryption algorithm operated at a
4 reception side are obtained from the transmission side and
5 when different encryption algorithms are operated at the
6 transmission side and the reception side, an encryption
7 algorithm operated at the transmission side is encrypted
8 with an encryption algorithm operated at the reception side
9 and transmitted to the reception side.

1 3. A cryptographic communication method as claimed in claim
2 2 wherein signature data produced based on a public key
3 preliminarily allocated to the transmission side is
4 supplied to the reception side with said encrypted
5 encryption algorithm.

02
1 4. A cryptographic communication method as claimed in claim
2 2 wherein signature data produced based on a public key
3 preliminarily allocated to the transmission side is
4 supplied to the transmission side together with said
5 encrypted encryption algorithm and transmitted to the
6 reception side.

1 5. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:

4 from a user of a transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side; and

7 querying a data base in which a correspondence between
8 the user identifier indicating the user and an encryption
9 algorithm operated by the user is preliminarily described
10 about each user and then retrieving the encryption
11 algorithm operated by the user of the transmission side and
12 the encryption algorithm operated by the user of the
13 reception side,

14 wherein if the encryption algorithm operated by the user of
15 the transmission side is different from the encryption
16 algorithm operated by the user of the reception side, data
17 indicating the encryption algorithm operated by the user of
18 the transmission side is encrypted with the encryption
19 algorithm operated by the user of the reception side and

20 transmitted to the user of the reception side.

1 6. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:

4 from a user of transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side;

7 querying a data base in which a correspondence between
8 user identifier indicating the user, an encryption
9 algorithm operated by the user and an encryption key is
10 preliminarily described about each user so as to obtain the
11 encryption algorithm operated by the user of the
12 transmission side and an encryption key thereof and an
13 encryption algorithm operated by the user of the reception
14 side and encryption key thereof,

15 wherein if the encryption algorithm operated by the user of
16 the transmission side is different from the encryption
17 algorithm operated by the user of the reception side, data
18 indicating the encryption algorithm operated by the user of
19 the transmission side and encryption key produced based on
20 the encryption key operated by the user of the reception
21 side corresponding to a key length of the encryption
22 algorithm is encrypted with the encryption algorithm
23 operated by the user of the reception side and transmitted
24 to the user of the reception side.

Q2

7. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and the encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data obtained by encrypting the encryption algorithm operated by the user of the transmission side with the encryption algorithm operated by the user of the reception side and signature data produced for the encryption key operated by the user of the reception side are transmitted to the user of the reception side.

8. An encryption algorithm sharing management method for sharing the encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between the user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data indicating the encryption algorithm operated by the user of the transmission side and encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of the encryption algorithm is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of

27 the reception side with the signature data produced
28 corresponding to the encryption key operated by the user of
29 the reception side.

1 9. Network communication system composed by connecting a
2 plurality of users, comprising at least an encryption key
3 management station to be connected from a user of a
4 transmission side,

5 said encryption key management station obtaining, from
6 the user of the transmission side, information indicating
7 an encryption algorithm operated by the user and
8 information indicating the encryption algorithm operated by
9 the user of the reception side and if different encryption
10 algorithms are operated by users of the transmission side
11 and a reception side, encrypting the encryption algorithm
12 operated by the user of the transmission side with an
13 encryption algorithm operated by the user of the reception
14 side and transmitting it to the user of the reception side.

1 10. Network communication system composed by connecting a
2 plurality of users, comprising at least an encryption key
3 management station to be connected from a user of a
4 transmission side,

5 said encryption key management station comprising a
6 data base in which a correspondence between a user
7 identifier indicating a user and an encryption algorithm

8 operated by the user is preliminarily described about each
9 user;

10 wherein

11 when a communication is carried out from the user of
12 the transmission side to a user of a reception side, a user
13 identifier indicating the user and a reception side user
14 identifier are obtained from the user of the transmission
15 side and said data base is queried with the obtained
16 identifier as a key so as to obtain an encryption algorithm
17 operated by the user of the transmission side and an
18 encryption algorithm operated by the user of the reception
19 side, and

20 if the encryption algorithm operated by the user of
21 the transmission side is different from the encryption
22 algorithm operated by the user of the reception side, the
23 encryption algorithm operated by the user of the
24 transmission side is encrypted with the encryption
25 algorithm operated by the user of the reception side and
26 transmitted to the user of the reception side.

1 11. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:

4 from a user of a transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side;

02
7 querying a data base in which a correspondence between
8 the user identifier indicating the user and an encryption
9 algorithm operated by the user is preliminarily described
10 about each user so as to retrieve an encryption algorithm
11 operated by the user of the transmission side and an
12 encryption algorithm operated by the user of the reception
13 side; and

14 if the encryption algorithm operated by the user of
15 the transmission side is different from the encryption
16 algorithm operated by the user of the reception side, data
17 indicating the encryption algorithm operated by the user of
18 the transmission side is encrypted with the encryption
19 algorithm operated by the user of the reception side and
20 transmitted to the user of the reception side.

1 12. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:

4 from a user of a transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side; and

7 querying a data base in which a correspondence between
8 the user identifier indicating the user, an encryption
9 algorithm operated by the user and an encryption key
10 thereof is preliminarily described about each user so as to
11 obtain the encryption algorithm operated by the user of the

12 transmission side and an encryption key and the encryption
13 algorithm operated by the user of the reception side and an
14 encryption key,

15 wherein if the encryption algorithm operated by the user of
16 the transmission side is different from the encryption
17 algorithm operated by the user of the reception side, data
18 indicating the encryption algorithm operated by the user of
19 the transmission side and the encryption key produced based
20 on the encryption key operated by the user of the reception
21 side corresponding to a key length of the encryption
22 algorithm is encrypted with the encryption algorithm
23 operated by the user of the reception side and transmitted
24 to the user of the reception side.

1 13. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:

4 from a user of a transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side; and

7 querying a data base in which a correspondence between
8 the user identifier indicating the user, an encryption
9 algorithm operated by the user and an encryption key is
10 preliminarily described about each user so as to obtain the
11 encryption algorithm operated by the user of the
12 transmission side and an encryption key thereof and the

13 encryption algorithm operated by the user of the reception
14 side and an encryption key thereof,
15 wherein if the encryption algorithm operated by the user of
16 the transmission side is different from the encryption
17 algorithm operated by the user of the reception side,
18 signature data produced for the encryption key operated by
19 the user of the transmission side is transmitted to the
20 user of the transmission side and the encryption algorithm
21 operated by the user of transmission side is encrypted with
22 the encryption algorithm operated by the user of the
23 reception side and transmitted to the user of the reception
24 side with the signature data produced for the encryption
25 key operated by the user of reception side.

1 14. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:
4 from a user of a transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side; and
7 querying a data base in which a correspondence between
8 the user identifier indicating the user, an encryption
9 algorithm operated by the user and an encryption key is
10 preliminarily described about each user so as to obtain the
11 encryption algorithm operated by the user of the
12 transmission side and an encryption key thereof and the

13 encryption algorithm operated by the user of the reception
14 side and an encryption key thereof,
15 wherein if the encryption algorithm operated by the user of
16 the transmission side is different from the encryption
17 algorithm operated by the user of the reception side,
18 signature data produced for the encryption key operated by
19 the user of the transmission side is transmitted to the
20 user of the transmission side and data indicating the
21 encryption algorithm operated by the user of the
22 transmission side and the encryption key produced based on
23 the encryption key operated by the user of the reception
24 side corresponding to a key length of the encryption
25 algorithm is encrypted with the encryption algorithm
26 operated by the user of the reception side and transmitted
27 to the user of the reception side with signature data
28 produced corresponding to the encryption key operated by
29 the user of the reception side.

1 15. Network communication system composed by connecting a
2 plurality of users, comprising at least an encryption key
3 management station to be connected from a user of a
4 transmission side,

5 said encryption key management station obtaining, from
6 the user of the transmission side, information indicating
7 an encryption algorithm operated by the user and
8 information indicating an encryption algorithm operated by

a2
9 a user of a reception side, and when different encryption
10 algorithms are operated by the user of the transmission
11 side and the user of the reception side, encrypting the
12 encryption algorithm operated by the user of the
13 transmission side with the encryption algorithm operated by
14 the user of the reception side and transmitted to the user
15 of the reception side.

16. Network communication system composed by connecting a
2 plurality of users, comprising at least an encryption key
3 management station to be connected from a user of a
4 transmission side, said encryption key management station
5 comprising a data base in which a correspondence between a
6 user identifier indicating a user and an encryption
7 algorithm operated by the user is preliminarily described
8 about each user;

9 wherein

10 when a communication is carried out from the user of
11 the transmission side to a user of a reception side, a user
12 identifier indicating the user and a reception side user
13 identifier are obtained from the user of the transmission
14 side, and said data base is queried with the obtained
15 identifier as a key so as to obtain an encryption algorithm
16 operated by the user of the transmission side and an
17 encryption algorithm operated by the user of the reception
18 side, and

19 if the encryption algorithm operated by the user of
20 the transmission side is different from the encryption
21 algorithm operated by the user of the reception side, the
22 encryption algorithm operated by user of transmission side
23 is encrypted with the encryption algorithm operated by the
24 user of the reception side and transmitted to the user of
25 the reception side.

1 17. A cryptographic communication method wherein if
2 different encryption algorithms are operated by a
3 transmission side and a reception side, an encryption
4 algorithm operated by the reception side is encrypted with
5 an encryption algorithm operated by the transmission side
6 and transmitted to the reception side.

1 18. A cryptographic communication method wherein
2 information indicating an encryption algorithm operated by
3 a transmission side and information indicating an
4 encryption algorithm operated by a reception side are
5 obtained from the transmission side and when different
6 encryption algorithms are operated by the transmission side
7 and the reception side, the encryption algorithm operated
8 by the reception side is encrypted with the encryption
9 algorithm operated by the transmission side and transmitted
10 to the transmission side.

1 19. A cryptographic communication method as claimed in
2 claim 18 wherein signature data produced based on a public
3 key preliminarily allocated to the reception side is
4 supplied to the transmission side with the encrypted
5 encryption algorithm.

20
1 20. An encryption algorithm sharing management method for
2 sharing an encryption algorithm for cryptographic
3 communication, comprising the steps of:

4 from a user of a transmission side, obtaining a user
5 identifier indicating the user and a user identifier
6 indicating a user of a reception side;

7 querying a data base in which a correspondence between
8 the user identifier indicating the user and an encryption
9 algorithm operable by the user is preliminarily described
10 about each user so as to obtain an encryption algorithm
11 operable by the user of the transmission side and an
12 encryption algorithm operable by the user of the reception
13 side;

14 determining whether or not there is an encryption
15 algorithm operable by the user of the transmission side and
16 the user of the reception side commonly; and

17 if the commonly operable encryption algorithm exists,
18 it is notified the user of the transmission side that
19 cryptographic communication at the user of the transmission
20 side and the user of the reception side is enabled.

1 21. An encryption algorithm sharing management method as
2 claimed in claim 20 wherein:

3 if the commonly operable encryption algorithm exists,
4 information indicating the encryption algorithm is
5 transmitted to the user of the transmission side and

6 if the commonly operable encryption algorithm exists,
7 it is notified the user of the reception side that
8 cryptographic communication at the user of the transmission
9 side and the user of the reception side is disabled.

1 22. An encryption algorithm conversion method for
2 converting an operating first encryption algorithm to other
3 second encryption algorithm comprising:

4 querying a data base in which a correspondence between
5 a user identifier indicating a user, an encryption
6 algorithm operated by the user and an encryption key is
7 preliminarily described with a user whose encryption
8 algorithm is to be converted with a key so as to obtain a
9 first encryption algorithm operated by the user and a first
10 encryption key; and

11 with a first management secret key preliminarily
12 allocated for management and operated on the first
13 encryption algorithm, supplying first and second signature
14 data written in the first and second encryption keys,
15 public key data obtained by encrypting a second public key
16 corresponding to a second management secret key operated on

17 the second encryption algorithm preliminarily allocated for
18 management with the first encryption algorithm, a second
19 encryption algorithm encrypted with the first encryption
20 algorithm and signature data produced based on the second
21 management secret key to the user.